

GDB: USAO 2019R00215

FILED ENTERED
LOGGED RECEIVED

JUL 23 2020

AT GREENBELT
CLERK U.S. DISTRICT COURT
DISTRICT OF MARYLAND

DEPUTY

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA

v.

JOEL ANTHONY SUPER,

Defendant

*
*
*
*
*
*
*

CASE NO. 20-mj-1787-TJS

FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT AND ARREST WARRANT

I, Jeffrey Starnes, being duly sworn, hereby depose and state as follows:

Introduction

1. I make this affidavit in support of a criminal complaint and arrest warrant.
2. Based on the following facts, there is probable cause to believe that on or about October 10, 2019, in the District of Maryland and elsewhere, **JOEL ANTHONY SUPER** ("SUPER") committed bank fraud, in violation of 18 U.S.C. § 1344.
3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this investigation.
4. The facts, conclusions, and beliefs I express in this affidavit are based on my training, experience, knowledge of the investigation, and reasonable inferences I've drawn from my training, experience, and knowledge of the investigation.

Agent Background

5. I am an “investigative or law enforcement officer of the United States” within the meaning of 18 U.S.C. § 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of and make arrests for offenses enumerated in 18 U.S.C. § 2516.

6. In my capacity as a United States Postal Inspector, I investigate allegations of criminal fraud involving the use of the United States mail. As a United States Postal Inspector and previously as a Special Agent for the United States Secret Service, I have gained experience investigating mail fraud, wire fraud, bank fraud, identity theft, investment fraud, credit card fraud, counterfeit securities and currency, false identification documents, and mortgage fraud.

Probable Cause

The Telfair Boulevard Search Warrant

7. On February 4, 2020, investigators from the Charles County Sheriff’s Office (“CCSO”) executed a Maryland state search warrant at **SUPER**’s apartment on Telfair Boulevard in Camp Springs, Maryland (“the Telfair Boulevard residence”).

8. Evidence found during the search included more than 100 personal and business checks that were from and made payable to individuals other than **SUPER**, blank check stock used to manufacture checks, a stolen United States Postal Service (“USPS”) arrow key, bank cards in the names of individuals other than **SUPER**, Social Security cards in the names of individuals

other than **SUPER**, driver's licenses in the names of individuals other than **SUPER**, and a Taurus PT111 model handgun bearing serial number TYK55598.¹

9. Once investigators entered **SUPER**'s residence, they observed an individual—later identified as **SUPER**—exit the bedroom window and jump from the balcony of the apartment, which is a one-bedroom unit on the second floor of the building.

10. Investigators identified the individual who jumped from the apartment as **SUPER** when they found **SUPER** on the ground with evidence of bank fraud, including stolen checks (one of which was drawn from the bank account of Victim 2, described below) and bank cards in the names of people other than **SUPER**.

11. Investigators identified **SUPER** as the only occupant of the one-bedroom residence. The investigators who executed the search warrant encountered only **SUPER**, there was only one bed in the Telfair Boulevard apartment, and the clothing in the apartment appeared to belong to one person. Moreover, while executing the warrant, investigators observed mail matter directed to **SUPER**.

12. At the conclusion of the search, officers from CCSO arrested **SUPER** on state offenses.

¹ USPS arrow keys ("arrow keys") are keys issued to and utilized by USPS employees to open USPS arrow locks ("arrow locks"). Arrow keys are unique silver metal keys that have the letters "USPS" above an arrow imprinted on one side and a series number and unique serial number imprinted on the opposite side. The series number is between one and three numeric digits, and the unique serial number is between four and five numeric digits. Arrow locks can be found on USPS collection boxes, apartment panel boxes, and central neighborhood mailboxes. In general, each series arrow key will open the corresponding series arrow locks within a geographic area. By policy, USPS employees are prohibited from possessing arrow keys outside the scope of their employment. Those who do not work for the USPS also are prohibited from possessing arrow keys. This stolen arrow key could open USPS collection boxes in Waldorf, Maryland.

13. Investigators contacted the management staff at the Telfair Boulevard apartment building, who provided records showing that the leaseholder of the Telfair Boulevard apartment was Individual C, who is **SUPER**'s mother.² No other individuals were listed on the lease. The apartment management also told investigators that they believed Individual C's son, who they identified as "**JOEL SUPER**," was living in the Telfair Boulevard residence and that **SUPER** recently attempted to obtain two new parking permits for the complex.

14. When **SUPER** attempted to obtain parking permits for the Telfair Boulevard apartment complex, **SUPER** gave the apartment management two fraudulent vehicle registrations showing that the registered owner of both vehicles was Individual C, who **SUPER** described to the management as his mother. Maryland Motor Vehicle Administration records show that the vehicle registrations—bearing Maryland tags 3DZ5588 and 7DF4923—were not registered to Individual C, but in fact were registered to **SUPER** and a relative of **SUPER**, Individual D.

The Defendant

15. **SUPER** has a criminal history that includes several convictions for fraud.

16. In January 2017, **SUPER** was found guilty of possession of a forged instrument in New York, New York.

17. In two cases in July and October 2017, **SUPER** was found guilty of access device fraud in separate jurisdictions in Pennsylvania, including East Whiteland Township and Montgomery Township, Pennsylvania.

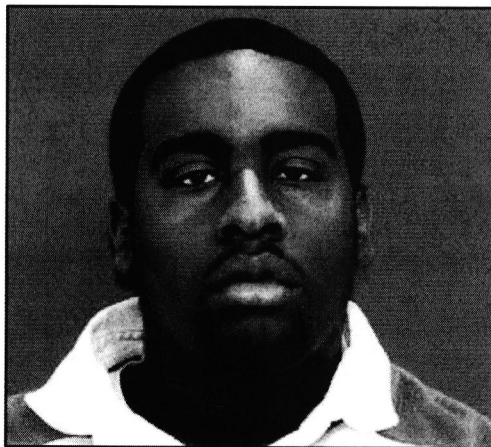
18. In February 2019, **SUPER** was found guilty of credit card larceny and identity theft in Virginia. For that conviction, **SUPER** received a sentence of three years' incarceration with all but four months suspended.

² **SUPER**'s probation officer confirmed that Individual C is **SUPER**'s mother.

19. **SUPER** has a pending case in Connecticut involving the theft and negotiation of a stolen check.

20. **SUPER** is currently on supervised probation for his conviction in Virginia. I spoke to **SUPER**'s probation officer on April 20, 2020, who confirmed that she spoke to **SUPER** earlier that day and that **SUPER** told the probation officer that he was in New York.

21. I obtained a Maryland driver's license image for **SUPER**, which is depicted below.



Victim 1

22. On October 12, 2019, Victim 1 reported to CCSO unauthorized activity with two of his bank accounts.³

23. On October 7, 2019, Check 3621—drawn from Victim 1's SunTrust Bank account ending in 2008 ("SunTrust 2008")—was deposited into a Chartway Federal Credit Union account ending in 0408 ("CFCU 0408"). The deposited check was in the amount of \$13,812 and was payable to Individual A.⁴ Victim 1 reported to investigators that he did not authorize the deposit

³ Victims are referred to using male pronouns, regardless of gender.

⁴ All amounts are rounded down to the nearest dollar.

of this check and that his checkbook contained checks in the 3400-number range, far below the check number on the fraudulent check to Individual A that was deposited into CFCU 0408.

24. Victim 1 also reported fraud involving his second bank account, a SunTrust Bank account ending in 6913 (“SunTrust 6913”). On October 10, 2019, a \$55,000 wire was electronically transmitted from SunTrust 6913 to an account with State Farm Bank. Victim 1 did not authorize this transaction.

25. Investigators identified internet protocol (“IP”) address 69.143.31.93 (“the 3193 IP address”) as the IP addressed used to access Victim 1’s SunTrust Bank accounts online.

26. Comcast records show that at the time of the fraudulent activity involving Victim 1’s SunTrust Bank accounts, the 3193 IP address was assigned to the Comcast internet account at **SUPER**’s apartment (the Telfair Boulevard residence).⁵ Those records also show that the phone number assigned to the internet account at **SUPER**’s residence was another certain telephone number ending in 6132 (“the 6132 number”).

27. Records associated with CFCU 0408—the account used to receive the fraudulent wire transfer from Victim 1’s SunTrust Bank account—show that the account was opened on September 12, 2019, under the name of Individual A. The phone number listed on the account is the 6132 number, and the address on the account is an apartment building in New York, New York. Further, the identification used to open the account was a fraudulent New York driver’s license that displayed a photograph of Individual D, not Individual A.

28. Those records also show that the 3193 IP address—the same IP address used to access Victim 1’s SunTrust Bank accounts without authorization, and the same IP address that was assigned to **SUPER**’s apartment—accessed CFCU 0408 on October 7, 8, and 9, 2019.

⁵ The account was opened in the name of Individual B.

29. During the February 4, 2020, search of **SUPER**'s apartment, investigators found a Social Security card displaying the name of Individual A and a certain Social Security number. This Social Security number was used to open CFCU 0408, the account used to receive the fraudulent \$55,000 wire from Victim 1's SunTrust bank account.

Stolen Checks

30. Investigators found more than 100 stolen personal and business checks in **SUPER**'s possession during the February 4, 2020, search of the Telfair Boulevard residence. Several of those checks were drawn from accounts that belonged to individuals and businesses residing and conducting business in Waldorf, Maryland. Investigators spoke to several of those victims.

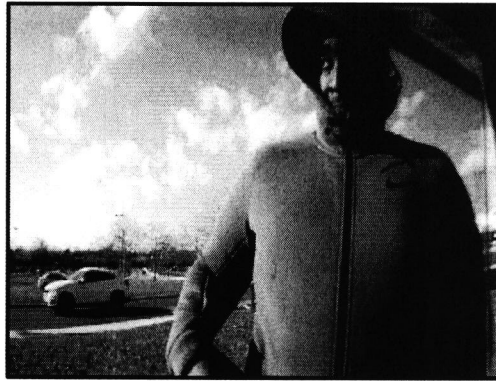
31. Victim 2—a resident of Waldorf, Maryland—discovered that he had been defrauded when he noticed that his bank account balance was lower than it should have been. According to Victim 2, he wrote Check 5783 from his SunTrust Bank account ending in 2821 ("SunTrust 2821") for \$20 to Company 1 in New York and sent the check to Company 1 through the mail, though the check never reached Company 1. Check 5783 was stolen and altered to reflect an amount of \$5,700 and a payee of Individual E. Investigators found Check 5783 in **SUPER**'s apartment on February 4, 2020. The check had been endorsed with Individual E's name.

32. Records show that this check was mobile-deposited into a Bethpage Federal Credit Union account ending in 1184 ("BFCU 1184") on December 17, 2019. Records associated with BFCU 1184 show that the account was opened on September 17, 2019, under the name Individual E.

33. The records associated with BFCU 1184 show at least one other suspicious check deposit. In particular, on December 9, 2019, a check in the amount of \$3,250 was mobile-deposited

into BFCU 1184 from an Interior Federal Credit Union account ending in 0011 (“IFCU 0011”), an account that belongs to Victim 3, who resides in Waldorf, Maryland.

34. On at least two occasions, the debit card for BFCU 1184—a debit card ending in 6371—was used to make cash withdrawals at automated teller machines (“ATMs”). On December 18, 2019, \$300 was withdrawn from BFCU 1184 at an M&T Bank ATM located at 10410 Campus Way South, Largo, Maryland. Surveillance footage of the transaction appears to depict **SUPER** wearing a Nike jacket with a zipper and hoodie (“the Nike jacket”) while conducting the transaction.



35. The debit card connected to BFCU 1184 was also used to make a \$300 cash withdrawal on December 17, 2019, at a Bank of America branch in Temple Hills, Maryland. Surveillance footage of this transaction, shown below, depicts an individual wearing what appears to be the Nike jacket that **SUPER** wore when he withdrew \$300 from BFCU 1184 at the M&T Bank ATM.



36. Investigators spoke with Victim 4, whose check was found at **SUPER**'s residence during the Telfair Boulevard search warrant. Victim 4's check was also endorsed.

37. Victim 4 mailed Check 2110 from his residential mailbox in Waldorf, Maryland, to pay his mortgage company. Victim 4 later discovered that Check 2110 had been stolen and altered to be made payable to Individual F for \$3,200. The check was drawn from Victim 4's Old Line Bank account ending in 8806 ("Old Line Bank 8806").

38. Bank records show that Check 2110 was mobile-deposited into a Discover Bank account ending in 2741 ("Discover Bank 2741") on February 3, 2020, the day before the search of the Telfair Boulevard residence. Records from Discovery Bank show that Discover Bank 2741 was opened on January 14, 2020, in the name of Individual F.

39. Additional stolen checks that were (a) found during the February 4, 2020, search of **SUPER**'s residence and (b) endorsed are described in the following table.

| <i>Victim</i> | <i>Victim Location</i> | <i>Victim Bank</i> | <i>Account No.</i> | <i>Check</i> | <i>Amount</i> |
|---------------|------------------------|--------------------|--------------------|--------------|---------------|
| 5 | Tennessee | First Tennessee | 3475 | 2554 | \$5,350.00 |
| 6 | New York | Bank of America | 5556 | 20874756 | \$4,970.62 |
| 7 | Florida | Seacoast Nat. Bank | 3371 | 7985 | \$7,695.27 |
| 8 | Maryland | SunTrust Bank | 8367 | 2004 | \$4,900 |
| 9 | Maryland | Old Line Bank | 1806 | 10154 | \$3,750 |
| 10 | Maryland | Old Line Bank | 9012 | 34380 | \$2,998 |

40. During the search of the Telfair Boulevard residence, investigators also found an ATM receipt dated September 16, 2019, for a check in the amount of \$11,700 that was deposited into an M&T Bank account ending in 9304 ("M&T Bank 9304") at a branch located in Clinton, Maryland. Records obtained from M&T Bank show that the check was drawn from a Bank of America bank account ending in 1459 ("BOA 1459") that belonged to Victim 11. The check was made payable to Individual G with an address in Laurel, Maryland. The phone number listed on BOA 1459 is the 6132 number.

41. On February 21, 2020, Victim 12, who resides in Brandywine, Maryland, reported that he mailed a check (Check 3244) for \$150 to a family member who resides in Waldorf, Maryland. The check was drawn from Victim 12's SunTrust Bank account ending in 8619 ("SunTrust 8619"). Victim 12 later discovered that the check was stolen and altered.

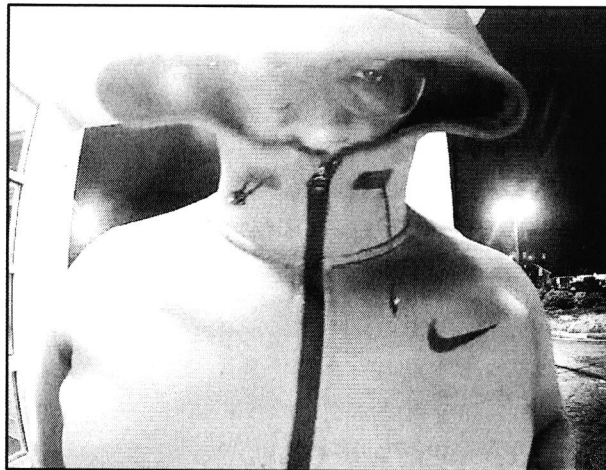
42. Check 3244 was altered to \$5,500 and the payee was changed to Individual H. Records show that on January 7, 2020, Check 3244 was deposited into a Bank of America account ending in 3699 ("BOA 3699") at a branch located in Temple Hills, Maryland. Bank records show that BOA 3699 was opened on November 6, 2019, in the name of Individual H. Surveillance footage of Check 3244 being deposited on January 7, 2020, depicts an individual wearing what appears to be the Nike jacket.



43. Records associated with BOA 3699 show five additional suspicious checks deposited into BOA 3699 that were drawn from accounts that belonged to Victims 13 through 17, in the aggregate amount of \$16,547, between November 21 and December 23, 2019.

44. One of those suspicious checks (Check 1733) was drawn from Victim 16's account with Treasury Department Federal Credit Union ending in 6247 ("TDFU 6247"). On December 9, 2019, Check 1733 was made payable to Individual H in the amount of \$3,250 and deposited into BOA 3699. The location of the deposit was in Oxon Hill, Maryland.

45. Surveillance footage of the deposit shows what appears to be **SUPER** wearing the Nike jacket while conducting the transaction.



46. Another one of the checks (Check 4385) deposited into BOA 3699 was drawn from Victim 17's account with Trustmark National Bank ending in 9789 ("Trustmark 9789"). Check 4385 was made payable to Individual H in the amount of \$2,800 and was deposited into BOA 3699 on December 23, 2019. The location of the check deposit was New York, New York.

47. Surveillance footage of the deposit shows an individual who appears to be **SUPER** wearing the Nike jacket while conducting the transaction.



48. Additional surveillance footage from BOA shows what appears to be **SUPER** wearing the Nike jacket and conducting withdrawals from BOA 3699 on January 3, 2020, at a branch in Temple Hills, Maryland, and again on January 4, 2020, at a branch in New York City, New York.

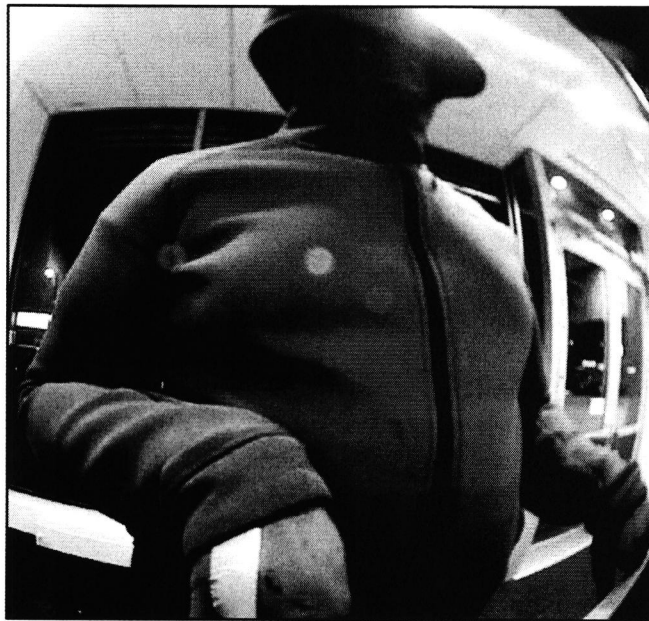


49. During the February 4, 2020, search of **SUPER**'s residence (the Telfair Boulevard residence), investigators found a cashier's check that was made payable to Individual B in the amount of \$108.

50. Records show that this check was deposited into a Santander Bank account ending in 6996 ("SB 6996"). The account was opened on October 7, 2019, under the name Individual B, and the phone number on the account was listed as the 6132 number.

51. The cashier's check was mobile-deposited on October 14, 2019. A review of the records for SB 6996 show that on October 30, 2019, a suspicious check (Check 2084) in the amount of \$8,500 was deposited into SB 6996. Check 2084 was drawn from Victim 18's JP Morgan Chase Bank account ending in 2106. Victim 18 resides in Armonk, New York.

52. Surveillance footage from Santander Bank depicts what appears to be **SUPER** wearing the Nike jacket while depositing Check 6996 on October 30, 2019, at a branch located in New York, New York.



The Connecticut Case

53. In April 2020, **SUPER** was arrested in Wilton, Connecticut, for depositing a stolen check. Victim 19 of Wilton, Connecticut, previously reported that he mailed a check (Check 1807) in the amount of \$735 to his insurance company. Victim 19 later discovered that Check 1807 had been stolen, altered to \$5,300, and made payable to Individual E.

54. Records show that on September 25, 2019, Check 1807 was deposited into a SunTrust Bank account ending in 1687 ("SunTrust 1687"), an account opened on August 27, 2019, in the name of Individual E.

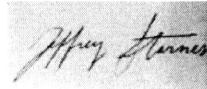
55. Surveillance footage from SunTrust Bank appears to depict **SUPER** depositing Check 1807 on September 25, 2019, at a SunTrust Bank branch located in Washington, D.C.



Conclusion

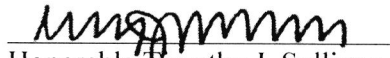
56. Based on the foregoing facts, there is probable cause to support the issuance of the requested criminal complaint and arrest warrant.

Respectfully submitted,



Inspector Jeffrey Starnes
United States Postal Inspection Service

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 4(d) this 20th day of July, 2020.



Honorable Timothy J. Sullivan
United States Magistrate Judge